Journal of Law and Policy

Volume 25 | Issue 1 Article 12

12-2-2016

Cellphones and the Fourth Amendment: Why Cellphone Users Have a Reasonable Expectation of Privacy in their Location Information

Paul Cividanes

CELLPHONES AND THE FOURTH AMENDMENT: WHY CELLPHONE USERS HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR LOCATION INFORMATION

*Paul Cividanes**

The Fourth Amendment, which affords individuals protection from unreasonable searches and seizures, was ratified over two hundred years ago. As such, it was impossible for the Amendment's framers to conceive the technologies that exist today. As technology progresses, courts are often faced with the task of deciding how the Fourth Amendment should apply in the modern world. As Fourth Amendment jurisprudence has developed, the Supreme Court has originated tests and doctrines for courts to use when hearing Fourth Amendment challenges to government action. One such test, the "reasonable expectation of privacy" test, looks to see whether an individual has a reasonable expectation of privacy in what the government has searched or seized. If the individual does in fact have such an expectation, law enforcement can search and/or seize that item only if they have a warrant, with some exceptions. One doctrine the court has announced, the third-party doctrine, stands for the proposition that individuals do not have a reasonable expectation of privacy in information they voluntarily convey to third parties. Cellphones, and similar devices the Framers never could have imagined, are now capable of revealing users' location information. This Note argues that Fourth Amendment protections should be extended to location information. Ultimately, cellphone users do not voluntarily convey their location information to third parties and therefore have a reasonable expectation of privacy in this information.

INTRODUCTION

The first mobile phone call was made on April 3, 1973 by Motorola senior engineer Martin Cooper to inform a rival telecommunications company that he was making the call via a mobile phone.[1] Mr. Cooper made the call on the Motorola DynaTac which was released for sale in 1983, weighed nearly two pounds, allowed thirty minutes of talk time and eight hours of standby, could store up to thirty phone numbers, and cost nearly $4,000.[2] The earliest cellphones were primarily capable of only making and receiving calls, and were mainly used for business, as opposed to personal use.[3] Mobile phone technology started to improve in the 1990s and it became more common for the average consumer to have a cellphone.[4] Eventually, the cellphone's purpose began to shift from a "verbal communication tool to a multimedia tool."[5] Today, cellphones weigh mere ounces and can often replace other gadgets such as cameras and music players.[6] Cellphones additionally

---

* J.D. Candidate, Brooklyn Law School, 2017. Thank you to my family, friends, and girlfriend Lauryn for always supporting me. Thank you to everybody on the *Journal of Law and Policy* and Professor Baer for all of their suggestions and contributions made while writing and editing this Note.

[1] Richard Goodwin, *The History of Mobile Phones From 1973 to 2008: The Handsets That Made It All Happen*, KNOW YOUR MOBILE (Apr. 16, 2015), http://www.knowyourmobile.com/nokia/nokia-3310/19848/history-mobile-phones-1973-2008-handsets-made-it-all-happen.

[2] *See id.*; *Evolution of Cell Phone Technology*, ENGINEERING & TECH. HIST. WIKI, http://ethw.org/Evolution_of_Cell_Phone_Technology (last modified Oct. 8, 2014); Nicole Nguyen, *The Evolution of the Cell Phone – How Far It's Come!*, READWRITE (July 4, 2014), http://readwrite.com/2014/07/04/cell-phone-evolution-popsugar.

[3] Amanda Ray, *The History and Evolution of Cell Phones*, ART INSTITUTES BLOG (Jan. 22, 2015), https://www.artinstitutes.edu/about/blog/the-history-and-evolution-of-cell-phones.

[4] Goodwin, *supra* note 1.

[5] Ray, *supra* note 3.

[6] *Id.*; *Evolution of Cell Phone Technology*, *supra* note 2; *see* Kara Cullen, *History of Cellphone Technology*, QRREADERS.NET, http://www.qrreaders.net/articles/history-cellphone-technology.html (last visited Oct. 10, 2016); *see also* Riley v. California, 134 S. Ct. 2473, 2490 (2014) (noting that there are over a million apps for such things as political news, addictions, dating, buying or selling items and other personal hobbies).

include features such as text messaging, email, Internet, the ability to update one's social media status, and access to a mobile application market that has "transformed the phone into a virtual toolbox with a solution for almost every need."[7] There are currently an estimated 207.2 million cellphone users in the United States.[8]

Another feature of modern cellphones is location-based services.[9] Location-based services allow cellphone users to share their location with friends on services such as Google Plus and Foursquare.[10] Despite some of these apps featuring the option to turn off location services,[11] cellphone companies are constantly recording users' locations,[12] a feature that "*cannot* be turned off."[13] One way cellphone companies record their users' locations is by keeping historical cell site location information ("CSLI") records.[14] Every time a person sends or receives a phone call, text message, email, or uses data, a record is kept of which cell tower their phone

---

[7] Ray, *supra* note 3; *see Riley*, 134 S. Ct. at 2490; Cullen, *supra* note 6; *Evolution of Cell Phone Technology*, *supra* note 2.

[8] *Number of Smartphone Users in the United States From 2010 to 2018 (In Millions)*, STATISTA, http://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/ (last visited Oct. 10, 2016).

[9] Kathryn Zickhur, *Location-Based Services*, PEW RES. CTR. (Sept. 12, 2013), http://www.pewinternet.org/2013/09/12/location-based-services/.

[10] *Id.*; *see* Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES (Mar. 26, 2011), http://www.nytimes.com/2011/03/26/business/media/26privacy.html.

[11] *See* Zickhur, *supra* note 9 (noting that cellphone users report they have "turned off location-tracking features at some point").

[12] Cohen, *supra* note 10.

[13] *Cell Phone Location Tracking Public Records Request*, ACLU (Mar. 25, 2013) (emphasis added), https://www.aclu.org/cases/cell-phone-location-tracking-public-records-request [hereinafter *Cell Phone Location Tracking*]; *see also* Amy Gahran, *Survey: Most Cell Phone Users Don't Protect Mobile Privacy*, CNN (Sept. 5, 2012), http://www.cnn.com/2012/09/05/tech/mobile/pew-mobile-privacy-gahran/ ("[R]egardless of whether you turn off location tracking on your phone, your wireless carrier knows (and keeps a record of) where your phone is at all times it's connected to the cell network."); Cohen, *supra* note 10 ("[W]e are already being tracked whether we volunteer to or not.").

[14] Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, ATLANTIC (Apr. 14, 2016), http://www.theatlantic.com/technology/archive/2016/04/sixth-circuit-cellphone-tracking-csli-warrant/478197/.

connects to.[15] Every time a phone connects to a cell tower, a CSLI record is kept and stored by the cellphone company.[16] Consequently, the Government can procure CSLI records and use them against a criminal defendant to place them at or nearby a crime scene.[17]

Currently, CSLI is not given Fourth Amendment protection against unreasonable searches and seizures by any federal circuit. In *United States v. Davis*, the Eleventh Circuit Court of Appeals, relying on a recent Fifth Circuit decision and a federal statute,[18] held that the government's warrantless procurement of CSLI does not violate the Fourth Amendment.[19] The court reasoned that a person has "no subjective or objective reasonable expectation of privacy" in CSLI information.[20] Additionally, the court relied on the third-party doctrine, which states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" to find that a user does not have an expectation of privacy in CSLI records.[21] The court found that since the defendant knew his cellphone provider was keeping CSLI records, he could not claim any expectation of privacy.[22] The court also found that the government properly secured a court order under the Stored

---

[15] *See* State v. Earls, 70 A.3d 630, 637 (N.J. Sup. Ct. 2013) ("As mobile devices register with a cell site, make a call, or download data, they 'communicate' with a station through radio signal data that is collected and analyzed at the provider's cell towers.").

[16] *Id.* at 632; Tim Sheehan, Note, *Taking the Third-Party Doctrine Too Far: Why Cell Phone Tracking Data Deserves Fourth Amendment Protection*, 13 GEO. J. L. & PUB. POL'Y 181, 183 (2015).

[17] Law enforcement has used CSLI in criminal investigations to place robbery suspects at the scene of a crime. *See generally* United States v. Graham, 796 F.3d 332 (4th Cir. 2015) (holding that obtaining CSLI cell cite constitutes a search because the government is privy to information about the user's movements and personal habits); United States v. Davis 785 F.3d 498, 518 (11th Cir. 2015) (holding that a court order compelling a cellphone provider to produce CSLI records for a 67-day period did not violate the Fourth Amendment).

[18] *See Davis*, 785 F.3d at 509–11.

[19] *Id.* at 517.

[20] *Id.* at 511.

[21] *Id.* at 509 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

[22] *Id.* at 511.

Communications Act ("SCA") to procure the records at issue.[23] The court noted that:

> Under the SCA, Congress authorized the U.S. Attorney to obtain court orders requiring "a provider of electronic communication service . . . to disclose a record or other information to a subscriber" . . . [upon a showing] of "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought [] are relevant and material to an ongoing criminal investigation."[24]

For a brief moment, the Fourth Circuit gave CSLI Fourth Amendment protection in *United States v. Graham*.[25] The Fourth Circuit originally held that the government's warrantless procurement of CSLI violated the Fourth Amendment.[26] The court reasoned that cellphone users had a reasonable expectation of privacy in CSLI information and therefore inspection of such information required a warrant.[27] On rehearing *en banc*, however, the Fourth Circuit held that the Government's procurement of CSLI from the defendant's cellphone provider did not in fact violate the Fourth Amendment.[28] Similar to the Eleventh Circuit's holding in *Davis*, the court found that the third-party doctrine did apply to CSLI and found that cellphone users do not have a reasonable expectation of privacy in such information.[29] Similarly, the Fifth Circuit refused to afford cellphone users' Fourth Amendment protection in their

---

[23] *Id.*

[24] *Id.* at 505 (quoting 18 U.S.C. § 2703 (c)–(d) (2009)).

[25] *See generally* United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (finding no violation of defendants' Fourth Amendment right where the government received historical CSLI from defendants' cell phone provider without a warrant). The case was reheard after the government's petition seeking a rehearing en banc was granted. Orin Kerr, Opinion, *Fourth Circuit Grants Rehearing, Eliminates Split, on Cell-Site Surveillance*, WASH. POST (Oct. 29, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/10/29/fourth-circuit-grants-rehearing-eliminates-split-on-cell-site-surveillance/?utm_term=.ca9581a2c0cc.

[26] United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015), *vacated*, 824 F.3d 421 (4th Cir. 2016).

[27] *Id.* at 345.

[28] *Graham*, 824 F.3d at 424.

[29] *Id.* at 425, 428.

location information and found that users are aware that cellphone use results in a voluntarily conveyance of CSLI to cellphone providers.[30] These circuit opinions are illustrative of the prevailing thought among the circuits not to extend Fourth Amendment protection to the procurement of CSLI.

This Note argues that the third-party doctrine should be revisited in its application to CSLI as well as other modern technologies. CSLI is rarely *knowingly* volunteered to a third-party; as such, cellphone users do have a reasonable expectation of privacy in this information and the procurement of CSLI should require a warrant. Part I provides a brief overview of what CSLI is and how it is used. Part II outlines related Fourth Amendment jurisprudence, which serves as a foundation for how courts determine whether a search is unreasonable and therefore requires a warrant. Part III illustrates the origins of the third-party doctrine and its application. Part IV discusses recent circuit court opinions holding that CSLI is not protected under the Fourth Amendment. Part V demonstrates how people have a reasonable expectation of privacy in CSLI information on the grounds that such information can reveal intimate details about a person's life. Part VI argues that the third-party doctrine should not apply to CSLI. Part VII proposes solutions to the problems that arise from the application of the third-party doctrine in the modern world. The doctrine requires reevaluation to discern whether additional requirements or guidelines are necessary in order to preserve Fourth Amendment protections. Ultimately, courts should use a multifactor test to determine if the doctrine should apply.

I. CELL SITE LOCATION INFORMATION

A cellphone user's location is constantly recorded when the phone is on, whether the user voluntarily shares that information or not and even when the user is unaware that their location is being recorded.[31] Once a cellphone is turned on, it begins to search for and

---

[30] *See In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 613–15 (5th Cir. 2013).

[31] *See* State v. Earls, 70 A.3d 630, 641, 657 (N.J. Sup. Ct. 2013).

then connects to the cell site that will provide the strongest signal.[32] The process occurs automatically and every seven seconds cellphones search for the site with the strongest signal.[33] The process also occurs whenever a cellphone user makes a call, sends a text message, or connects to the Internet.[34] Cellphones can even be tracked when the user takes no action at all, so long as the phone is turned on.[35] Cellphone providers also record a cellphone's registration data, by producing a log of all the cell sites the cellphone has registered with.[36] All of this information is recorded in a database and a log is kept for each time a call is made or data is used which can be analyzed to approximate the phone's location at a particular time.[37] These records "comprise the bulk of CSLI."[38]

As cellphone use became more frequent, the placement of cell towers grew rapidly, leading to greater accuracy in location information.[39] The precision of recording a cellphone user's location varies depending on the size of the "cell sector," which is the overall area the cell tower covers.[40] Phones that are used "in smaller sectors can be located with greater accuracy than those in larger ones."[41] Historically, in the first cellular systems, the base stations were generally placed far apart, creating large cell sectors that could potentially cover an area several miles or more in diameter.[42] Due to today's ubiquitous use of cellphones, the size of cell sectors has generally decreased, as a sector can only handle so many connections in the limited amount of space allocated to a wireless

---

[32] *Id.* at 637.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *See id.*

[38] Elizabeth Elliot, *United States v. Jones: The (Hopefully Temporary) Derailment of Cell-Site Location Information Protection*, 15 LOY. J. PUB. INT. L. 1, 7 (2013).

[39] *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 12–30 (2010) [hereinafter *ECPA Reform*] (statement of Professor Matt Blaze).

[40] *Id.* at 23–24.

[41] *Id.* at 24.

[42] *Id.*

carrier within a given sector.[43] This has led to more cellular base stations with a corresponding decrease in the area served by each station.[44] As a result, carriers are able to locate users with greater precision and accuracy.[45]

CSLI data is constantly being collected by cellphone carriers.[46] During a criminal investigation, the government may seek disclosure of "historical" CSLI, "real time" CSLI, or both.[47] When the government obtains historical CSLI, they are given location information that already exists, and when they obtain real time CSLI information, they are given location information as soon as it becomes available to the phone provider.[48] As the government will ultimately obtain both from the cellphone provider, the distinction is of no real substance to the provider.[49] However, both forms of CSLI "become[] important in relation to the privacy interest" of the cellphone user.[50] Real time CSLI can be used by law enforcement to track a person's movements and locations as they are happening, whereas historical CSLI can be used to recreate a person's movements or place them at a certain location at a certain time.[51] There is a potential for abuse with access to this information, however, as an individual's locations and movements may reveal many intimate details about a person, leading one to have a

---

[43] *See id.*

[44] *Id.* at 25.

[45] State v. Earls, 70 A.3d 630, 632 (N.J. Sup. Ct. 2013).

[46] *See* Steven M. Harkins, Note, *CSLI Disclosure: Why Probable Cause is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE L. REV. 1875, 1883 (2011); *see also Earls*, 70 A.3d at 637 (noting that location information can be recorded whether the cell phone user is using the phone or not, so long as the phone is turned on).

[47] Harkins, *supra* note 46, at 1883.

[48] *Id.* at 1884.

[49] *Id.* at 1883–84.

[50] *Id.* at 1884.

[51] *See id.*; *see also Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 310–11 (2004) (describing how law enforcement was able to rebut Scott Peterson's statement that he left his house at 9:30 by introducing "cell phone records [that] placed him at home until 10:08").

reasonable expectation of privacy in such information.[52] Thus, the Fourth Amendment's protections against unreasonable searches and seizures should extend to CSLI.

II. FOURTH AMENDMENT JURISPRUDENCE

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[53]

One of the main concerns the Framers had when ratifying the Fourth Amendment was prohibiting the utilization of general warrants and writs of assistance that were used under English common law.[54] General warrants allowed the Crown's messengers to conduct a search without providing any reason or belief that someone had committed an offense.[55] Similarly, writs of assistance permitted a search for untaxed goods.[56] These practices were unsuccessfully challenged in court, and some, such as John Adams, considered this legal battle the "spark that led to the Revolution."[57] "Both controversies led to the famous notion that a person's home is their castle, not easily invaded by the government."[58] Since its

---

[52] *See* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (noting that location information can reveal a "wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations").

[53] U.S. CONST. amend. IV.

[54] Barry Friedman & Orin Kerr, *Common Interpretation – The Fourth Amendment*, NAT'L CONST. CTR., http://constitutioncenter.org/interactive-constitution/amendments/amendment-iv (last visited Oct. 10, 2016).

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id.*

ratification in 1791,[59] the Fourth Amendment has been the center of much debate among scholars and courts.

The Supreme Court originally took a property-based approach to interpreting Fourth Amendment protections.[60] Historically, "the sanctity of the home" has firmly been established, and is one of the oldest strains of Fourth Amendment law.[61] The Court has consistently used this doctrine throughout Fourth Amendment jurisprudence, "drawing a 'firm line'" at an individual's home and distinguishing privacy within the home and the public nature outside of it.[62] The Court can be somewhat particular about this line, as a search that occurs right outside the home, also known as curtilage, is afforded Fourth Amendment protections, while a search a little further away, considered to be outside of the curtilage, might not be afforded protection under the Fourth Amendment.[63] The property-based approach can be considered relatively simple as one can draw a "neat distinction between public and private."[64]

---

[59] *Id.*

[60] Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and The Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 258 (2016).

[61] *Id.*

[62] *Id.* (quoting Payton v. New York, 455 U.S. 573, 590 (1980)).

[63] *See id.* at 258–59. *Compare* Oliver v. United States, 466 U.S. 170, 180 (1984) ("At common law, the curtilage is the area to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life,' and therefore has been considered part of the home for Fourth Amendment purposes."), *and* Florida v. Jardines, 133 S. Ct. 1409 (2013) (holding that police bringing a drug-sniffing dog onto a man's porch is considered to be a search within the meaning of the Fourth Amendment and thus, given Fourth Amendment protection), *with* California v. Greenwood, 486 U.S. 35, 40 (1988) (holding that police going through garbage left outside of the curtilage is not protected under the Fourth Amendment because a person has no expectation of privacy in "garbage bags left on or at the side of a public street [that] are readily accessible to animals, children, scavengers, snoops and other members of the public"). The Court has provided four factors to consider when determining whether an area is within curtilage. *See* United States v. Dunn, 480 U.S. 294, 301 (1987) ("[C]urtilage questions should be resolved with particular reference to four factors: the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by.").

[64] Price, *supra* note 60, at 259.

When the Fourth Amendment was ratified in the eighteenth century,[65] it is unlikely that its drafters envisioned modern technological advancements of today. Thus, as new technologies began to emerge, the Court had to decide how the Fourth Amendment would apply in light of these new advancements. In 1928, the Supreme Court had to make such a decision in *Olmstead v. United States*.[66] In *Olmstead*, federal prohibition officers tapped the defendant's phone by placing wires along the ordinary telephone wires outside of his residence.[67] Strictly adhering to the property-based approach, the Court held that the wire-tapping at issue did not constitute a search under the Fourth Amendment, noting that the insertions were made without trespassing on the defendant's property.[68] The Court reasoned that the wires were not a part of the defendant's home or office,[69] declining to consider "how the technology worked and the role it played in society."[70] In his dissent in *Olmstead*, Justice Brandeis took issue with this approach, positing that the Constitution is in essence a living document that must be able to adapt to "a changing world."[71]

Subsequently, in *Goldman v. United States*, the Supreme Court ruled that law enforcement's use of a detectaphone—a device that is placed against a wall to pick up sounds—did not violate the Fourth

---

[65] Friedman & Kerr, supra note 54.

[66] *See generally* Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967) (addressing whether evidence obtained by secretly wiretapping a private phone call was done so in violation of the Fourth Amendment).

[67] *Id.* at 456–57.

[68] *Id.* at 465–66.

[69] *Id.* at 465.

[70] Price, *supra* note 60, at 260.

[71] *See* Olmstead, 277 U.S. at 472–73, *overruled by* Katz v. United States, 389 U.S. 347 (1967) (Brandeis, J., dissenting) ("Legislation, both statutory and constitutional, is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions and purposes. Therefore a principal to be vital must be capable of wider application than the mischief which gave it birth." (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

Amendment.[72] In *Goldman*, federal agents were given access to the defendant's neighboring office by the building's superintendent and placed the detectaphone against the partitioning wall.[73] The agents were then able to hear statements made by the defendant, which prosecutors later used against him for conspiracy to violate the Bankruptcy Act.[74] The Court refused to distinguish the wiretapping in *Olmstead* and the use of the detectaphone, adhering to Olmstead's property-based approach by noting that what was heard by the detectaphone was not a trespass.[75] The *Olmstead* and *Goldman* decisions were reflections of the Court's former refusal to give weight to new technology and how it functions in society and its general reluctance to expand beyond the property-based approach.[76]

In 1928, the year the Court decided *Olmstead*, there were approximately eighteen million phones being used in households within the United States.[77] By 1965, that number grew over five times.[78] Telephone use became a part of every-day life for Americans, which meant that the Court would need to seriously reconsider *Olmstead* if there was ever to be any privacy afforded to telephone use.[79] In 1967, the Court had the opportunity to do so when deciding *Katz v. United States*.[80] In *Katz*, FBI agents attached an electronic listening and recording device to a phone booth used by the defendant, which enabled them to overhear the calls he made.[81] The defendant insisted that the phone booth was a

---

[72] Goldman v. United States, 316 U.S. 129, 135 (1942), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

[73] *Id.* at 131–32.

[74] *Id.* at 130, 132.

[75] *Id.* at 134–35.

[76] *See* Price, *supra* note 60, at 260.

[77] *Id.* at 261 (citing U.S. CENSUS BUREAU, *in* COMMUNICATIONS 775, 783 (1970), http://www2.census.gov/prod2/statcomp/documents/CT1970p2-05.pdf.

[78] U.S. CENSUS BUREAU, *in* COMMUNICATIONS 775, 783 (1970), http://www2.census.gov/prod2/statcomp/documents/CT1970p2-05.pdf (noting there were approximately 93.7 million telephones in American homes in 1965).

[79] *See* Price, *supra* note 60, at 261.

[80] *Id.*

[81] Katz v. United States, 389 U.S. 347, 348 (1967).

"constitutionally protected area,"[82] however the lower court held that the recordings did not violate the Fourth Amendment on the grounds that there was "no physical entrance into the area occupied by[] the [defendant]."[83] On appeal, the Supreme Court found that the defendant incorrectly framed the issue and noted, "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.'"[84] The majority opinion concluded that, "the Fourth Amendment protects people, not places."[85] The Court further noted that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[86] The majority explicitly overruled *Olmstead* and *Goldman*, stating that the "'trespass' doctrine there enunciated can no longer be regarded as controlling,"[87] and went on to hold that the government's actions were in violation of the Fourth Amendment.[88]

While the home and other property is still sufficiently protected by the Fourth Amendment,[89] *Katz* was an important decision because it broadened Fourth Amendment protections and established that such protections are not merely dictated by property law.[90] While groundbreaking, the majority opinion did not provide much guidance to determine when such protections may exist.[91] However, Justice Harlan provided such guidance in his concurrence: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second,

---

[82] *Id.* at 351.

[83] *Id.* at 348–49.

[84] *Id.* at 350.

[85] *Id.* at 351.

[86] *Id.*

[87] *Id.* at 353.

[88] *See id.* at 359.

[89] *See* United States v. Jones, 132 S. Ct. 945, 951 (2012) ("*Katz* . . . established that 'property rights are not the sole measure of Fourth Amendment violations,' but did not 'snuf[f] out the previously recognized protection for property.'" (quoting Soldal v. Cook County, 506 U.S. 56, 64 (1992)).

[90] *See* Price, *supra* note 60, at 264.

[91] *Id.*

that the expectation be one that society is prepared to recognize as 'reasonable.'"[92] This two-part "reasonable expectation of privacy" test has become the "litmus test" of Fourth Amendment protection.[93]

In recent years, the Supreme Court has considered technological developments when deciding cases involving Fourth Amendment challenges. In *Kyllo v. United States*, the Court considered whether the government's use of a thermal imaging device to detect heat waves emanating from a defendant's home was a search in violation of the Fourth Amendment.[94] The Court considered not only the technology of the thermal imaging device at issue, but also other, "more sophisticated systems that [were] already in use or in development," and found that the government's warrantless use of the device violated the Fourth Amendment.[95] In *Riley v. California*, the Court was asked "to decide how the search incident to arrest doctrine applied to modern cellphones."[96] The Court considered the immense storage capacity that modern cellphones have, which can hold vast amounts of personal information, while further noting that location information derived from cellphones can precisely reconstruct a cellphone user's whereabouts.[97] As such, the Court held that the search incident to arrest doctrine does not allow law enforcement to search the digital contents of an arrestee's cellphone without a warrant.[98]

While the Court has yet to decide a case involving the procurement of CSLI, these recent decisions indicate that the Court will likely favorably consider technological progression when hearing Fourth Amendment challenges. The procurement of CSLI involves technology that the framers of the Fourth Amendment could never have imagined, and courts should take this into account when deciding whether to give CSLI Fourth Amendment protections.

---

[92] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[93] *See* Price, *supra* note 60 at 262.

[94] *See* Kyllo v. U.S., 533 U.S. 27, 29 (2001).

[95] *Id.* at 36–37, 40.

[96] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[97] *Id.* at 2489–90.

[98] *Id.* at 2493 (holding that it "is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest").

III. THE THIRD-PARTY DOCTRINE

The third-party doctrine, which has been implemented in criminal cases since the late 1970s, essentially establishes "that information lawfully held by many third parties is treated differently from information held by the suspect himself."[99] This information can be procured "by subpoenaing the third party, by securing the third party's consent or by any other means of legal discovery."[100] A third party can include "any non-governmental institution or entity established by law."[101] The two leading cases that established this doctrine are *United States v. Miller* and *Smith v. Maryland*.[102]

In *Miller*, the defendant was on trial for defrauding the United States of tax revenues, among other related charges.[103] Prior to trial, the defendant moved to "suppress copies of checks and other bank records obtained by . . . allegedly defective subpoenas . . . served upon two banks at which he had accounts."[104] The Court found that the District Court correctly denied the motion to suppress, as there was no intrusion into any area in which the defendant had a protected Fourth Amendment interest.[105] The Court noted that the defendant could not claim ownership or possession of the records at issue, finding that they were not the defendant's "private papers," but rather business records that belonged to the banks.[106] Since the documents contained information that was voluntarily conveyed to the banks, the Court found there was no legitimate "expectation of privacy" in such documents.[107] The Court also noted that an

---

[99] Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine be Revisited?*, A.B.A. J. (Aug. 01, 2012), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

[100] *Id.*

[101] Price, *supra* note 60, at 265.

[102] Kerr & Nojeim, *supra* note 99.

[103] United States v. Miller, 425 U.S. 435, 436 (1976).

[104] *Id.* The defendant claimed "the subpoenas were defective because they were issued by the United States Attorney rather than a court, no return was made to a court, and the subpoenas were returnable on a date when the grand jury was not in session." *Id.* at 438–39.

[105] *Id.* at 440.

[106] *Id.*

[107] *Id.* at 442.

individual assumes the risk when revealing certain information to others that it may be conveyed to the government, "even if that information was revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[108]

The Court expanded on the third-party doctrine in *Smith v. Maryland*, where a robbery victim was receiving menacing telephone calls from a man claiming to be the robber.[109] The police eventually discovered that the defendant was the one making the calls,[110] and "the telephone company, at the police's request, installed a pen register at its central offices to record the numbers dialed from the telephone" at the defendant's house.[111] The police did not have a warrant or court order directing the telephone company to install the pen register.[112] The police used the information recorded by the pen register to obtain a warrant to search the defendant's residence, which revealed evidence implicating him in the robbery.[113] The Supreme Court found that the defendant had no "legitimate expectation of privacy" in numbers dialed on a phone.[114] Similar to its holding in *Miller*, the Court noted that the pen register was installed on company property and therefore, the defendant could not claim that *his* property was invaded.[115]

The Court further distinguished the records at issue in *Katz* from the ones derived from a pen register and found that the listening device employed in *Katz* revealed *contents* of communications, whereas pen registers do not acquire any such content.[116] Instead, they disclose "only the telephone numbers that have been dialed—a

---

[108] *Id.* at 443.

[109] Smith v. Maryland, 442 U.S. 735, 737 (1979).

[110] *See id.* (noting that during one call, the caller asked the robbery victim to come outside, which allowed her to see the defendant's car, enabling the police to trace the license plate number to the defendant).

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.* at 745.

[115] *Id.* at 741.

[116] *Id.*

means of establishing communication."[117] The majority expanded on its reasoning as to why people have no expectation of privacy in the numbers they dial, explaining that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company," and they also are aware that the phone company keeps permanent records of such conveyances, albeit admitting that people may be uninformed of pen registers' mechanics.[118] Relying on *Miller*, the Court found that even if the defendant had a subjective expectation of privacy in the numbers he dialed, that expectation was not "one that society is prepared to recognize as 'reasonable,'"[119] because a "person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[120] The Court further held that when the defendant "voluntarily conveyed numerical information to the telephone company," he assumed the risk of the company possibly disclosing the numbers he dialed to the police.[121]

While the third-party doctrine has been criticized since its inception,[122] even stronger criticisms can be made in today's modern

---

[117] *Id.* (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977).

[118] *Id.* at 742 ("Although most people may be oblivious to a pen register's esoteric functions, they presumably have some common awareness of one common use: to aid in the identification of persons making annoying or obscene calls."); *see also* Stewart Baker, *Drawing a Line on the Third-party Doctrine*, WASH. POST (May 4, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/04/drawing-a-line-on-the-third-party-doctrine ("The theory of *Smith* is that I have a reduced privacy expectation in things [I have] shared with others.").

[119] *Smith*, 442 U.S. at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

[120] *Id.* at 743–45 (noting that the defendant voluntarily conveyed information to the telephone company that had facilities for recording and was free to record); *see* United States v. Miller, 425 U.S. 435 (1976).

[121] *Smith*, 442 U.S. at 744.

[122] *See id.* at 749 (Marshall, J., dissenting) (noting that even assuming that individuals typically know a phone company monitors calls for its own reasons, it does not follow that they expect this information to be made available to the general public or the government); *see also* United States v. Miller, 425 U.S. 435, 449 (1976) (Brennan, J., dissenting) ("A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. Thus, we hold petitioner had a reasonable expectation that the bank would maintain the confidentiality of those papers which originated with him in check form and of

world. The amount of data that third parties collect today is arguably "much more revealing than in the 1970s," when the doctrine was first articulated.[123] Third parties can also collect more information in today's world because more information is stored online.[124] In light of the differences in information that is revealed to third parties today, as compared to when the third-party doctrine was first developed, the Court should revisit the doctrine's application in order to ensure that advancements in technology do not erode Fourth Amendment protections.

IV. FEDERAL CIRCUIT DECISIONS ON CELL SITE LOCATION INFORMATION

Currently, CSLI is not given Fourth Amendment protection by any federal circuit. For a brief period of time, the Fourth Circuit held that CSLI is protected under the Fourth Amendment,[125] but that case was reheard and the original decision was vacated.[126] Similarly, both the Fifth and Eleventh Circuits have held that CSLI is not afforded Fourth Amendment protection.[127]

---

the bank statements into which a record of those same checks had been transformed pursuant to internal bank practice.").

[123] Kerr & Nojeim, *supra* note 99.

[124] *See id.*; *see also* Baker, *supra* note 118 (noting the mass amounts of data people share on the Internet, especially by way of using smart phones); Price, *supra* note 60, at 266 ("[M]odern technology has dramatically expanded the scope of the third-party doctrine to reach far beyond records of bank transactions and telephone calls."); Natasha H. Duarte, *The Home Out of Context: The Post-Riley Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1148 (2015) ("Now that most of our data is stored on third-party servers, the Third-party Doctrine has effectively removed vast amounts of digital data—much of which includes personal information—from Fourth Amendment protection.").

[125] United States v. Graham, 796 F.3d 332, 344–45 (4th Cir. 2015).

[126] United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016) ("A majority of the panel held that, although the Government acted in good faith in doing so, it had violated [d]efendant's Fourth Amendment rights when it obtained the CSLI without warrant . . . . We now hold that the Government's acquisition of historical CSLI from [d]efendant's cell phone provider did not violate the Fourth Amendment.").

[127] *See generally* United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (holding that an individual has no reasonable expectation of privacy in CSLI and

In *United States v. Davis*, the Eleventh Circuit Court of Appeals considered whether CSLI should be given Fourth Amendment protection.[128] The government, using the SCA, acquired a court order compelling a robbery suspect's cellphone provider to disclose sixty-seven days' worth of CSLI.[129] The defendant's motion to suppress this evidence, arguing that the "records constituted a search under the Fourth Amendment and thus required probable cause and a search warrant," was denied.[130] At trial, the police produced a map showing the precise locations of the robberies as well as the cell towers that connected the defendant's calls around the time of the robberies.[131]

The Eleventh Circuit held that the court order for the production of the records at issue did not violate the Fourth Amendment.[132] Similar to *Miller*, the court noted that the defendant could neither claim ownership nor possession of the third-party's CSLI business records.[133] The court also found that CSLI does not contain a cellphone user's private information as it is essentially "non-content evidence."[134] The court, relying on the third-party doctrine and the Supreme Court's reasoning in *Smith* and *Miller*, found that the defendant had no subjective or objective reasonable expectation of privacy in the CSLI records.[135] The court reasoned that a cellphone user has no subjective expectation of privacy because they know they transmit signals to cell towers within the range of where the cellphone is used, that the cell tower functions as the equipment that connects the calls, that when users are making or receiving a call

---

therefore its procurement is not protected under the Fourth Amendment); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 613–15 (5th Cir. 2013) (finding that a cellphone user is aware that CSLI is voluntarily conveyed to a cellphone provider and is therefore not afforded Fourth Amendment protections).

[128] *See generally* United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (holding that a court order compelling third-party business records containing CSLI for a 67-day period did not violate Fourth Amendment rights).

[129] *Id.* at 501–02.

[130] *Id.* at 503.

[131] *Id.* at 501.

[132] *Id.* at 511.

[133] *Id.*

[134] *Id.* (emphasis omitted).

[135] *Id.*

they are exposing their general location, and that cellphone companies keep records of such cell tower usage.[136]

The court also concluded that cellphone users do not have an objective expectation of privacy in CSLI.[137] The majority rejected both the defendant's and dissent's reliance on the concurrences in *United States v. Jones*, in which it was argued that CSLI is the equivalent to GPS monitoring and thus requires the government to show probable cause.[138] The court distinguished GPS and CSLI, noting that CSLI is less precise and that reasonable expectations of privacy "do not turn on the quantity of non-content information" the cellphone provider collected in CSLI records.[139] Although the court did admit that technology has evolved since the days of *Smith* and *Miller*, it concluded that CSLI should not be given Fourth Amendment protection due to the third-party doctrine's exclusionary effect.[140] The court also recognized the pervasive use of cellphones and the fact that some users may want to stop cellphone providers from compiling location information or producing it to the government, but stated that such proposals should be directed to Congress rather than the courts.[141]

Similarly, the Fifth Circuit found that cellphone users have an awareness and understanding that cellphone use results in a voluntary conveyance of CSLI to cellphone providers and refused to afford users Fourth Amendment protection in their location information.[142]

In *United States v. Graham*, the Fourth Circuit originally held that the government's warrantless procurement of a robbery

---

[136] *Id.*

[137] *Id.* (noting that cellphone users know about publicly available information regarding technologies and practices that phone companies use so they should be aware of how cell towers function and that providers record such cell tower usage).

[138] *Id.* at 514; *see also* United States v. Jones, 132 S. Ct. 945 (2012) (holding that law enforcement violated the Fourth Amendment when they placed a GPS tracking device on a suspect's vehicle without a proper warrant).

[139] *Davis*, 785 F.3d. at 515.

[140] *Id.* at 512.

[141] *Id.* at 532.

[142] *See In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 613–15 (5th Cir. 2013).

suspects' historical CSLI was an unreasonable search and therefore violated the Fourth Amendment.[143] The Court discussed how "[e]xamination of a person's historical CSLI . . . [allows] the government to trace the movements of the cell phone . . . user," which would enable them to "discover the [user's] private activities and personal habits."[144] The court concluded that "cell phone users have an objectively reasonable expectation of privacy in this information [and] [i]ts inspection by the government, therefore, requires a warrant, unless an established exception to the warrant requirement applies."[145] The majority discussed how a Fourth Amendment search can be achieved through inspection of third-party records and decided that the third-party doctrine should not apply to CSLI[146] because "cell phone users do not voluntarily convey their CSLI to their service providers."[147] Further, the court explained how the third-party doctrine could hamper Fourth Amendment rights and expectations of privacy as technology continues to evolve.[148]

After the government asked the court to rehear the case en banc, the Fourth Circuit held that the Government's procurement of CSLI from the defendant's cellphone provider did not in fact violate the Fourth Amendment.[149] Similar to the Eleventh Circuit, the court found that the third-party doctrine did apply to CSLI and that cellphone users do not have a reasonable expectation of privacy in such information.[150]

Ultimately, courts should use the Fourth Circuit's original reasoning in *Graham*, and hold that CSLI should be protected under the Fourth Amendment. CSLI reveals private details about an

---

[143] *See* United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015).

[144] *Id.* at 345.

[145] *Id.*

[146] *See id.* at 351–52.

[147] *Id.* at 353–55 (noting some reasons why cell phone users do not voluntarily convey CSLI, including: service providers automatically generate the records, a user is not required to actively submit any location information when using their phone and some cell phone users are not generally aware that the records are being generated).

[148] *See id.* at 358–60.

[149] United States v. Graham, 824 F.3d 421, 424, 437–38 (4th Cir. 2016).

[150] *Id.* at 428.

individual which gives cellphone users a reasonable expectation of privacy in such information.[151] Additionally, the third-party doctrine should not apply to the procurement of CSLI as it can be reasoned that cellphone users are not *knowingly* and *voluntarily* providing third parties with this information.[152]

V. CELLPHONE USERS HAVE A REASONABLE EXPECTATION OF PRIVACY IN CSLI RECORDS

Location information can reveal private information about an individual.[153] The Supreme Court decision in *United States v. Jones*, although dealing with GPS records rather than CSLI,[154] emphasized how location data can reveal private information about an individual. In *Jones*, government agents installed a GPS tracking device on the defendant's vehicle without a valid warrant.[155] The majority opinion strictly adhered to the property-based approach to the Fourth Amendment, holding that because "[t]he government physically occupied private property for the purpose of obtaining information," the use of the GPS device on the defendant's vehicle to monitor its movements, constituted a search under the Fourth Amendment.[156] It was Justice Sotomayor's concurring opinion, however, that illustrated just how much information location data can reveal.[157] Justice Sotomayor explained that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial,

---

[151] *See infra* Part V.

[152] *See infra* Part VI.

[153] *See* United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring).

[154] *See generally Jones*, 132 S. Ct. 945 (deciding a case where law enforcement officers placed a GPS tracking device on defendant's automotive vehicle).

[155] *See id.* at 948 (noting that the government did obtain a warrant to use a tracking device, but did not follow the geographic or temporal limitations of the warrant).

[156] *Id.* at 949.

[157] *See id.* at 955–56 (Sotomayor, J., concurring).

political, professional, religious, and sexual associations."[158] The information that is revealed from GPS monitoring can essentially be equated with the information CSLI reveals, or any other location data type record. In fact, "[g]iven the ubiquity of cell phones and the fact people carry them almost everywhere they go—including inside a home—cell site information can be even more revealing than GPS information."[159] Either way, no matter the source, location data reveals the same information—your location. And this location information, no matter the source, reveals a variety of personal details about an individual.[160]

Such information can paint a detailed portrait of one's life, revealing things such as when a person comes and goes and whether they spent the night at home or elsewhere.[161] Location information can essentially reveal our various patterns of movement and who we associate with.[162] These recorded interactions can also lead to inferences about an individual's religious beliefs, sexual orientation, and political affiliations.[163] Certain inferences from location information can be made; for example, a few visits to a doctor specializing in treating a certain condition can lead to the conclusion

---

[158] *Id.* at 955 (Sotomayor, J., concurring). GPS, and location data in general, can also reveal information such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Id.* at 955 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

[159] Hanni Fakhoury, *From California to New York, Cell Phone Location Records are Private*, ELECTRONIC FRONTIER FOUND. (June 16, 2015), https://www.eff.org/deeplinks/2015/06/california-new-york-cell-phone-location-records-are-private [hereinafter Fakhoury, *From California to New York*]; *see also* Commonwealth v. Augustine, 4 N.E.3d 846, 861 (Mass. 2014) ("[T]here is a strong argument that CSLI raises even greater privacy concerns than a GPS tracking device. In contrast to such a device attached to a vehicle, because a cellular telephone is carried on the person of its user, it tracks the user's location far beyond the limitations of where a car can travel." (citation omitted)).

[160] *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (noting some establishments individuals visit which can be revealed through location information).

[161] Fakhoury, *From California to New York*, *supra* note 159.

[162] *See id.*

[163] *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

that an individual has that condition.[164] While it can be argued that a one-time revelation of an individual's location may not reveal much about a person, multiple trips to a doctor or gynecologist, for example, coupled with frequent trips to stores catering to new mothers and infants could reveal that a woman is pregnant, a fact she may deem private and not want to share with others. It is the revelation of an individual's location taken in the aggregate that begins to paint a picture of one's private life.

When the government procures CSLI an individual's location is not being revealed merely once, but rather at high volumes, revealing months' worth of a person's movements.[165] Courts sometimes look at this under what has been termed the "mosaic theory," where they review the government's collective action as a whole, rather than looking at individual steps.[166] Under this approach, the collective action observed as a whole could constitute a search whereas an individual action looked at in isolation would not.[167] This theory more suitably protects cellphone users' privacy expectations in CSLI, as individuals may be less concerned about their location being revealed only once, as opposed to their every move being revealed for weeks or months at a time. When location

---

[164] *See* Elizabeth Dwoskin, *What Secrets Your Phone is Sharing About You*, WALL STREET J. (Jan. 13, 2014), http://www.wsj.com/articles/SB10001424052702303453004579290632128929194. Further inferences can be made, such as revealing sensitive political information, showing certain leaders meeting, who may be involved and when and where they gather. A person's romantic life can be revealed by tracking the location of cell phones at night. *See* Jane Mayer, *What's the Matter with Metadata*, NEW YORKER (June 6, 2013), http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata.

[165] *See Jones*, 132 S. Ct. at 948; United States v. Davis, 785 F.3d 498, 501–02 (11th Cir. 2015); United States v. Graham, 796 F.3d 332, 349–50 (4th Cir. 2015). In *Jones*, law enforcement generated over two thousand pages of location data through its GPS monitoring of the suspect. *Jones*, 132 S. Ct. at 948. In *Davis*, law enforcement procured sixty-seven days' worth of location information from a suspect's cellphone provider. *Davis* 785 F.3d at 501–02. In *Graham*, law enforcement procured two hundred twenty-one days' worth of location information from a suspect's cellphone provider, revealing over twenty-eight thousand location data points. *Graham*, 796 F.3d at 349–50.

[166] Orin S. Kerr, *The Mosaic Theory of The Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2013).

[167] *See id.* at 328.

information is aggregated over long periods of time, as opposed to an individual location, intimate and private details about one's life can be revealed. As such, one would have a reasonable expectation of privacy in this information.

As location information reveals intimate details about one's life, "it [is] clear that people . . . [would expect] location information . . . to remain private" even when it is stored by cellphone providers.[168] A 2014 study has further shown that "Americans expect privacy in the data stored . . . and generated by their cellphones, including location information."[169] According to that study, 82 percent of Americans consider information revealing their location to be even more sensitive than "their relationship history, religious or political views, or the content of their text messages."[170]

Of course, there are those who are less guarded about sharing private or personal information with their social media friends and followers.[171] However, there is a difference between the location information one chooses to broadcast on social media, such as going

---

[168] Hanni Fakhoury, *A National Consensus: Cell Phone Location Records Are Private*, ELECTRONIC FRONTIER FOUND. (July 29, 2014), https://www.eff.org/deeplinks/2014/07/constitutionally-important-consensus-location-privacy [hereinafter Fakhoury, *A National Consensus*]; *see also* Brief for Electronic Frontier Foundation as Amicus Curiae Supporting Appellant, United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (No. 12-12928), 2014 WL 7006395 at 6 (en banc) (citing Dave Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTE: PRIVACY BLOG (Sept. 5, 2013), http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-usersmore-concerned-about-mobile-privacy-than-brand-or-screen-size; JANICE Y. TSAI ET AL., CARNEGIE MELLON UNIV., LOCATION-SHARING TECHNOLOGIES: PRIVACY RISKS AND CONTROLS 12 (2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf) (noting that a significant number of cell phone users did not like the idea of being tracked and some believe that the risks of location sharing outweigh the benefits resulting in a concern about controlling who can access their location information).

[169] Brief for Electronic Frontier Foundation as Amicus Curiae Supporting Appellant, *Davis*, 785 F.3d 498 (No. 12-12928), 2014 WL 7006395 at 5 (citing MARY MADDEN, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA, PEW RES. CENTER 36–37 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf).

[170] *Id.* (citing MADDEN, *supra* note 169, at 36–37).

[171] Fakhoury, *A National Consensus*, *supra* note 168.

to a concert at the park to see the latest band, and the information revealed from CSLI, such as going to the doctor, spending the night at a mistress' house, or any other place one would like to keep private.[172] The former is information people may actually want to share with others, or at the very least may not mind if it is revealed to the public, while the latter is information that one may hope remains private. CSLI does not distinguish between the two forms and reveals all location information that is stored by the cellphone provider.

Many cellphone users are taking affirmative steps to keep their location information private,[173] evidencing that they have a reasonable expectation of privacy in location data. Although some individuals broadcast their location to the world by posting pictures or using social media, there are many people who not only make sure that they do not post such information, but take steps to ensure that companies do not gain access to certain information they deem private.[174] Studies reveal that some cellphone users will not use an app when they realize how much personal information must be disclosed in order to use it.[175] Studies also show that cellphone users are turning off location tracking features.[176] While the CSLI tracking

---

[172] *See id.*

[173] *See* Brief as Amicus Curiae Supporting Appellant, *supra* note 169, at 5–6 (citing LAUREN BOYLES ET AL., PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES, PEW RES. CTR. 8–9 (Sept. 5, 2012), http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf).

[174] BOYLES ET AL., *supra* note 173, at 2 ("Many cell phone users take steps to manage, control, or protect the personal data on their mobile devices.").

[175] *See id.* ("54% of app users have decided to not install a cell phone app when they discovered how much personal information they would need to share in order to use it . . . 30% of app users have uninstalled an app that was already on their cell phone because they learned it was collecting personal information that they [did not] wish to share . . . . Taken together, 57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons.").

[176] *See id.* ("19% of cell owners have turned off the location tracking feature on their cell phone because they were concerned that other individuals or companies could access that information."); Zickhur, *supra* note 9 ("[A]lmost half (46%) of teen app users say [that] they have turned off the location tracking feature on their cell phone or in an app on a phone or tablet because they were worried about other people or companies being able to access that information . . . . [O]ver a third (35%) of adult cell app users said they have turned off the location-tracking feature on their cell phones.").

function of cellphones cannot be turned off,[177] the fact that people are taking affirmative steps to prevent location information from being made public illustrates that cellphone users maintain an expectation of privacy in such records. Although this information is exposed to the cellphone providers, a cellphone user's subjective expectation of privacy is not diminished for this reason, and cellphone users can still maintain an objective expectation of privacy in location information, effectively satisfying the test set out in *Katz*.[178]

Increasingly more states have attested that cellphone users have a reasonable, objective expectation of privacy in CSLI. A number of state legislatures are now requiring warrants for location data records, as well as CSLI.[179] Several state courts have also ruled that CSLI and other location information is essentially private information that people have a reasonable expectation of privacy in,

---

[177] *See Cell Phone Location Tracking*, *supra* note 13 ("All cell phones register their location with cell phone networks several times a minute, and this function cannot be turned off while the phone is getting a wireless signal."); *see also* Amy Gahran, *supra* note 13 ("[R]egardless of whether you turn off location tracking on your phone, your wireless carrier knows (and keeps a record of) where your phone is at all times it's connected to the cell network."); Cohen, *supra* note 10 (noting that cell phone users are continuously being tracked whether they volunteer to or not).

[178] *See* Brief for Electronic Frontier Foundation as Amicus Curiae Supporting Appellant, *supra* note 168.

[179] *See* Fakhoury, *A National Consensus*, *supra* note 168. "Hawaii, New York, Oregon and Washington require police to [obtain] a search warrant to track a person's movement using GPS or other electronic tracking device." *Id.* After the concurring opinions in *United States v. Jones* recognized that people can expect information about their movements will remain private, "Colorado, Maine, Minnesota, Montana and Utah passed statutes requiring law enforcement to use a search warrant to obtain historical cell site information. Indiana, Virginia, and Wisconsin" require law enforcement to obtain "a warrant . . . to track a cell phone in real time." *Id.* Riverside County, California, Denver, Wichita and Lexington, Kentucky require police to show probable cause and obtain a warrant when they track mobile phones. *Cell Phone Location Tracking*, *supra* note 13. The California legislature is also considering legislation "that would require police to obtain a warrant to get location records and other kinds of digital data." Fakhoury, *From California to New York*, *supra* note 159.

and therefore should be protected by the Fourth Amendment.[180] For instance, in *People v. Weaver*, the New York Court of Appeals ruled that the government infringed a burglary suspect's reasonable expectation of privacy in his location information by placing a GPS tracking device on his vehicle.[181] As one can conclude that CSLI contains more revealing information than GPS, the court's reasoning is applicable to CSLI as well.[182] In *State v. Earls*, the New Jersey Supreme Court held that its State Constitution "protects an individual's privacy interest in the location of his or her cellphone," and "users are reasonably entitled to expect confidentiality in the ever-increasing level of detail that cellphones can reveal about their lives."[183] In *Commonwealth v. Augustine*, the Massachusetts Supreme Court noted that historical CSLI allows the government to "track and reconstruct a person's past movements, a category of information that *never* would be available through the use of traditional law enforcement tools of investigation."[184] The court held that the defendant had satisfied the *Katz* "reasonable expectation" test by showing that he had a subjective expectation of privacy interest that "society is prepared to recognize as reasonable" in the location information revealed in the CSLI records.[185] Similarly, in *Tracey v. State*, the Florida Supreme Court held that CSLI implicates both a subjective expectation of privacy and one that "society is now prepared to recognize as objectively reasonable

---

[180] Lauren E. Babst, Note, *No More Shortcuts: Protect Cell Site Location Data With a Warrant Requirement*, 21 MICH. TELECOMM. TECH. L. REV. 363, 382 (2015).

[181] People v. Weaver, 909 N.E.2d 1195, 1201 (N.Y. 2009).

[182] Fakhoury, *From California to New York*, *supra* note 159 ("*Weaver* should apply to cell site location records too, regardless of the fact that the cell phone service providers hold the records. Given the ubiquity of cell phones and the fact people carry them almost everywhere they go—including inside a home—cell site information can be even more revealing than GPS information.").

[183] State v. Earls, 70 A.3d 630, 644 (N.J. 2013) ("Because of the nature of the intrusion, and the corresponding, legitimate privacy interest at stake, [the court held] . . . that police must obtain a warrant based on a showing of probable cause, or qualify for an exception to the warrant requirement, to obtain tracking information through the use of a cell phone.").

[184] Commonwealth v. Augustine, 4 N.E.3d 846, 865 (Mass. 2014).

[185] *Id.* at 856–57.

under the *Katz* 'reasonable expectation of privacy test.'"[186] The fact that many states are providing location privacy protections to its citizens through statutes and court decisions illustrates that it is reasonable to expect this location information to remain private.[187] Admittedly, states can afford more protection than the U.S. constitutional baseline,[188] and "[w]hile the Fourth Amendment does not depend on state law or statutory guarantees, they are nonetheless compelling evidence of societal understandings of privacy."[189] The decisions made by state courts and legislatures provide strong support for the assertion that cellphone users do, in fact, have an objective expectation of privacy in CSLI and similar location information.

Location data can reveal very personal details about one's life, details that users expect to remain private. Although there is no option to prevent cellphone companies from recording CSLI, cellphone users are taking affirmative steps to prevent their location information from being made public.[190] Additionally, state courts and legislatures are expressly telling people that they have a reasonable expectation of privacy through statutes and court decisions. These trends demonstrate that cellphone users have a reasonable expectation of privacy in CSLI and similar location information and procurement of such information should therefore require a warrant.

---

[186] Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (quoting Katz v. United States, 389 U.S. 347, 360–61 (1967)).

[187] *See* Fakhoury, *From California to New York*, *supra* note 159.

[188] *See* People v. Weaver, 909 N.E.2d 1195, 1202 (N.Y. 2009).

[189] Fakhoury, *A National Consensus*, *supra* note 168.

[190] *See* BOYLES ET AL., *supra* note 174 ("19% of cell owners have turned off the location tracking feature on their cell phone because they were concerned that other individuals or companies could access that information."); *see also* Zickhur, *supra* note 9 ("[A]lmost half (46%) of teen app users say that they have turned off the location tracking feature on their cell phone or in an app on a phone or tablet because they were worried about other people or companies being able to access that information . . . . [O]ver a third (35%) of adult cell app users said they have turned off the location-tracking feature on their cell phones.").

VI. THE THIRD-PARTY DOCTRINE SHOULD NOT APPLY TO CELL SITE LOCATION INFORMATION

The third-party doctrine states "that information lawfully held by many third parties is treated differently from information held by the suspect himself."[191] Foundational case law for the doctrine has articulated that, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[192] The underlying theory of the third-party doctrine is that an individual has a "reduced privacy expectation in things [they have] shared with others."[193] This theory has been criticized since the doctrine was first introduced.[194] Presumably, most individuals would not expect that information they share with others would be shared with law enforcement. It would not follow that, because CSLI is produced to the cellphone companies, you would have a reduced expectation of privacy in those records. Further, it is reasonable to expect that the company will not share your location with others, unless they are ordered to do so after being presented with a warrant. Another issue is whether cellphone users voluntarily give these records over to the cellphone company. CSLI is automatically generated and produced to the phone company,[195] and it is questionable whether users are even aware that this process is taking place.

---

[191] Kerr & Nojeim, *supra* note 99.

[192] United States v. Graham, 796 F.3d 332, 352–53 (4th Cir. 2015) (quoting Smith v. Maryland, 442 U.S. 735, 742 (1979)).

[193] Baker, *supra* note 118.

[194] *See* Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("[A]ssuming . . . that individuals 'typically know' that a phone company monitors calls for internal reasons . . . it does not follow that they expect this information to be made available to the public in general or the government."); United States v. Miller, 425 U.S. 435, 449 (1976) (Brennan, J., dissenting) ("A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. Thus, we hold petitioner had a reasonable expectation that the bank would maintain the confidentiality of those papers which originated with him in check form and of the bank statements into which a record of those same checks had been transformed pursuant to internal bank practice.").

[195] *See* State v. Earls, 70 A.3d 630, 636 (N.J. 2013).

The third-party doctrine does not categorically exclude all records from Fourth Amendment protection, but rather, the doctrine simply states that a person cannot claim a legitimate expectation of privacy in information that they voluntarily convey to third parties.[196] It is this voluntary conveyance that triggers an assumption of risk and reduced expectation of privacy.[197] CSLI records do not trigger this assumption of risk or reduced expectation of privacy because CSLI is automatically generated,[198] a feature that cannot be turned off by the cellphone user.[199] A cellphone user does not take any affirmative steps to disclose their location to their cellphone provider; rather, the company records users' location regardless of consent.[200] CSLI are records that simply wind up in the hands of a third party, not one in which a person voluntary conveys information. Also, CSLI is recorded when a user receives a call or text message.[201] In this case, a cellphone user is not affirmatively acting, much less making a voluntary conveyance.[202] The automatic generation of CSLI is no more than a byproduct of having a cellphone, and this act cannot be regarded as a voluntary conveyance triggering a reduced expectation of privacy.[203]

Another issue in the application of the third-party doctrine to CSLI records is whether cellphone users are even aware that such information is being generated. The Third Circuit has noted that, "it is unlikely that cell phone customers are aware that their cellphone providers collect and store historical location information."[204] Additionally, scholars have noted that, "[m]ost people are not aware of just how much data cellphone companies are storing and for how

---

196 *Graham*, 796 F.3d at 354.

197 *Id.*

198 *See Earls*, 70 A.3d at 637.

199 *Cell Phone Location Tracking*, *supra*, note 13; Gahran, *supra* note 13.

200 *See Graham*, 796 F.3d at 355.

201 *Id.*

202 *Id.*

203 *See* Babst, *supra* note 180, at 389.

204 In re United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3rd Cir. 2010).

long."[205] It is difficult to argue that a user voluntarily conveys information to a third party when he/she is unaware that such information is being conveyed at all.

A typical response to this argument is that cellphone users are given fair warning in their cellphone contracts that cellphone providers will collect location information and, if necessary, turn that information over to law enforcement.[206] This argument lacks merit however, on the ground that "studies have shown that users of electronic communications services often do not read or understand their providers' privacy policies."[207] In fact, even Chief Justice Roberts admits that he usually does not read user agreements necessary to access certain websites.[208] Moreover, cellphone companies do not typically disclose just how much information they actually collect,[209] and will not provide a cellphone user with their own location information even if requested.[210] It thus seems unlikely that cellphone users will have a true understanding of what information is being collected. Even if a cellphone user would like to analyze the location information cellphone companies collect, he/she will not be able to do so under current carrier practices.

---

[205] R. Craig Curtis et al., *Using Technology the Founders Never Dreamed Of: Cell Phones as Tracking Devices and The Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 63 (2014).

[206] *See* Babst, *supra* note 180, at 391.

[207] *Graham*, 796 F.3d at 345; *see also* FTC STAFF REPORT, FED. TRADE COMM'N, MOBILE POLICY PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 10 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (noting that consumers were not aware of how cellphone providers collect and use information derived from their cellphones); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L & POL'Y FOR INFO. SOC'Y 543, 544 (2009) (noting that privacy policies are often difficult to read and usually go unread).

[208] Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, A.B.A. J. (Oct. 20, 2014), http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/.

[209] Cohen, *supra* note 10.

[210] *See* Megha Rajagopalan, *Cellphone Companies Will Share Your Location Data – Just Not With You*, PRO PUBLICA (June 27, 2012), https://www.propublica.org/article/cellphone-companies-will-share-your-location-data-just-not-with-you.

Lastly, the third-party doctrine should be revisited, as its application in today's technologically advanced world may pose a threat to Fourth Amendment protections. Justice Sotomayor, in her concurring opinion in *Jones*, stated that the third-party doctrine approach is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[211] The third-party doctrine, established in the 1970s[212] during the Carter administration,[213] was introduced in the context of "analog-era,"[214] "primitive . . . technology," such as "a pen register that recorded the phone numbers a person dialed from a stationary phone."[215] The amount of data that winds up with third parties today is potentially much more revealing than when the doctrine was established in 1970.[216] Pen registers, the device at issue when the doctrine was first established, only reveal the phone numbers a user dialed;[217] CSLI can potentially track your every move.[218] This is problematic because, while some information can be deduced just by the numbers you dialed, such as perhaps a relationship with the user at the other end, knowing somebody's location and daily movements can reveal a wide range of intimate details about one's life. The doctrine also applies to the enormous amount of data that one shares on the Internet.[219] Today, most of our data is stored on a third-party server.[220] If all of this information can be obtained without a warrant, there is a grave risk that our Fourth Amendment privacy protections are effectively meaningless in the

---

[211] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[212] *See generally* United States v. Miller, 425 U.S. 435 (1976) (showing that this was the first case to fully assert the third-party doctrine); Smith v. Maryland, 442 U.S. 735 (1979) (applying the third-party doctrine to a technological device).

[213] *See* Fakhoury, *From California to New York*, *supra* note 159.

[214] *Id.*

[215] Cindy Cohn & Hanni Fakhoury, *With Third Party Records, Privacy Doesn't Require Secrecy*, ELECTRONIC FRONTIER FOUND. (May 7, 2015), https://www.eff.org/deeplinks/2015/05/third-party-records-privacy-doesnt-require-secrecy.

[216] Kerr & Nojeim, *supra* note 99.

[217] *Smith*, 442 U.S. at 741.

[218] Cohn & Fakhoury, *supra* note 215.

[219] *See* Baker, *supra* note 118.

[220] Duarte, *supra* note 124, at 1148.

context of information generated through different forms of modern technology.[221]

One may respond to these assertions by arguing that one can choose simply to not use a cellphone if they are concerned about their privacy, and if they do use a cellphone, they assume the risk that such information may be disclosed to law enforcement.[222] Cellphones, however, are ubiquitous[223] and now a "necessary part of [modern] life for many people."[224] "[T]oday, 90 percent of Americans carry cell phones."[225] Cellphones are "increasingly viewed as necessary to social interactions as well as the conduct of business."[226] The Supreme Court has even noted that, "cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[227] A 2013 study showed that cellphone users use their phone in almost any place and any time imaginable, including in the shower, during sex, and at church.[228] The only way to avoid disclosure of all the information cellphones

---

[221] *See* Baker, *supra* note 118; *see also* Hanni Fakhoury, *New Court Ruling Makes it Easier for Police to Track Your Cell Phone*, ELECTRONIC FRONTIER FOUND. (July 31, 2013), https://www.eff.org/deeplinks/2013/07/fifth-circuit-approves-warrantless-cell-phone-tracking [hereinafter Fakhoury, *New Court Ruling*] ("[T]he 'third party doctrine'—the idea you have no expectation of privacy in information turned over to third parties—is dangerously eroding our Fourth Amendment protection at a time when cell phone companies and Internet service providers are stockpiling extensive personal information about all of us.").

[222] *See In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013) (noting that cell phone use is not required by the government, but rather, is voluntary).

[223] *Planet of the Phones*, ECONOMIST (Feb. 28, 2015), http://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones.

[224] *Can You Imagine Life Without A Cell Phone?*, NORTHEAST TIMES (June 19, 2013), http://www.northeasttimes.com/2013/jun/19/can-you-imagine-life-without-cell-phone/#.V9sH5WXSeRs.

[225] Fakhoury, *A National Consensus*, *supra* note 168.

[226] Commonwealth v. Augustine, 4 N.E.3d 846, 859 (Mass. 2014).

[227] Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[228] HARRIS INTERACTIVE, JUMIO, 2013 MOBILE CONSUMER HABITS STUDY 3 (2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf.

reveal is essentially by not using one.[229] However, this is not a viable choice. It would be impractical for a person not to use a cellphone in present day society, and inaccurate to say that one assumes the risk when using a cellphone. In *Smith*, Justice Marshall noted in his dissent that "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[230] Justice Brennan made a similar finding in his dissent in *Miller* by recognizing that "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[231] In today's world, there is no practical alternative to using a cellphone if one wishes to actively participate in contemporary society.

Admittedly, the third-party doctrine does serve a legitimate purpose when applied in an appropriate context. The doctrine "ensures technological neutrality of the Fourth Amendment by blocking the opportunistic use of third parties to circumvent the basic balance of Fourth Amendment rules."[232] The use of third parties essentially has a "substitution effect" by allowing wrongdoers to take "public aspects of their crimes and replace them with private transactions," effectively allowing suspects to hide their criminal activities from public observation.[233] For example, a mob boss might have subordinates act through his orders, a stalker might call his victim rather than physically stalking her, and a computer hacker might infiltrate computers located miles away from his location.[234] In all of these scenarios, the wrongdoer is committing his crime through a third party while avoiding public detection.[235] The third-party doctrine prevents wrongdoers from evading detection through the use of third parties and properly preserves the

---

[229] State v. Earls, 70 A.3d 630, 641 (N.J. 2013).

[230] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[231] United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

[232] Orin S. Kerr, *The Case For The Third-party Doctrine*, 107 MICH. L. REV 561, 566 (2009).

[233] *Id.* at 573.

[234] *Id.* at 576.

[235] *Id.*

Fourth Amendment's balance between an individual's reasonable expectation of privacy and the government's interest in preventing criminal activity.[236]

There are notable differences between wrongdoers *knowingly* using third parties to commit crimes versus cellphone users, potentially *unknowingly*, generating CSLI or any other form of location information. Of course, a cellphone user could be discussing criminal activity on the call that generates the CSLI record. However, that information would be within the *content* of the call, and not produced by incidental CSLI records. The typical cellphone user generating CSLI is not acting through a third party to commit a crime while avoiding public detection.

Ultimately, the fact that CSLI is delivered to a third party should not diminish a cellphone user's reasonable expectation of privacy. A cellphone user is not knowingly and voluntarily conveying any information to a third party, and whether they know they are conveying the information or not, have no choice but to reveal this information to a third party. It is also questionable whether the doctrine is even compatible with modern technological advancements. Further, location information reveals intimate details about an individual's life.[237] As such, users have a reasonable expectation of privacy in these records.

VII. PROPOSED SOLUTIONS

Ultimately, courts should use a multifactor test before applying the third-party doctrine. Before applying the doctrine, courts should consider the following: (1) whether an individual *knowingly* conveys information to a third party; (2) whether the information was conveyed to a third party by a direct act of an individual or as a byproduct of a separate act; (3) whether an individual was using a third party during the commission of a crime; (4) the amount of intimate details revealed by the records at issue; and (5) the ubiquitous nature of the actions which led to information being

---

[236] *Id.* at 564.

[237] *See* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (noting that location information can reveal a "wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations").

released to a third party balanced against the practicality of abstaining from such an act. Using this multifactor test can truly preserve the spirit of the third-party doctrine, while adequately affording individuals Fourth Amendment protections.

One potential solution to the problems posed by the third-party doctrine is an elaboration or ruling on the doctrine stating that only records a person *knowingly* conveys to a third party will invoke the doctrine. Under this proposal, the true purpose of the doctrine can be preserved simultaneously with guaranteed Fourth Amendment protections; information that an individual knowingly and voluntarily turns over to third parties will not be afforded protection, while information that is unknowingly, and therefore not voluntarily conveyed, will still be afforded Fourth Amendment protection. This guarantees that certain information, such as CSLI, will be afforded protection under the Fourth Amendment. This standard, standing alone, could prove to be problematic, however, as it may prove too difficult to demonstrate what a person *knowingly* conveys to third parties, especially in the CSLI context.

In conjunction with the third-party doctrine applying only to information an individual *knowingly* turns over to third parties, an additional ruling that the doctrine will not apply to information that is generated as a byproduct of a separate act would also preserve the spirit of the third-party doctrine, while sufficiently affording Fourth Amendment protections. In other words, courts should look at how third parties obtain the information the government is seeking. The doctrine should apply only if the information was conveyed to a third party as a direct, affirmative act of an individual, not if the information was conveyed as a byproduct of a separate act. For instance, individuals directly convey their banking information to a third party when they hand a direct deposit slip to a teller; the depositor is committing a direct affirmative act in conveying information to the teller. However, individuals do not affirmatively convey their location information to a cellphone provider when they use their cellphone. Instead, the cellphone user's affirmative act is turning on their phone, making a phone call, or sending a text message; the generation of a CSLI record is no more than a byproduct of that affirmative act. Excluding the doctrine's application to information generated as a byproduct can preserve the purpose of both the Fourth Amendment and the third-party doctrine.

Another solution may be to apply the doctrine only when it can be determined that a suspect is using a third party during the commission of a crime. For instance, the court should apply the doctrine when a cellphone user makes calls to harass or threaten somebody, but not when a cellphone is being used for legitimate purposes, such as calling a friend or checking emails. This approach could preserve the balance between an individual's privacy interests, and the government's interest in preventing criminal activity.

Further building off *Riley* and Justice Sotomayor's concurrence in *Jones*, courts should consider the amount of intimate details that can be revealed by the information at issue. Cellphones have immense storage capacity and can contain a variety of personal information.[238] An individual's daily movements can also reveal very personal details.[239] The Court should then use a balancing test often utilized in Fourth Amendment cases, whereby the Court balances "the degree to which [the search] intrudes upon an individual's privacy and . . . the degree to which it is needed for the promotion of legitimate governmental interests."[240] Here, the procurement of CSLI is highly intrusive on individual privacy and the need for law enforcement to procure this information without a warrant is relatively low. The government could still obtain these records with a warrant if they have probable cause to do so, and it would be a relatively rare occurrence where it would be impractical for the government to obtain a warrant due to an immediately pressing exigency.

Finally, courts should consider the ubiquitous nature and necessity of an individual's action(s) that led to information being conveyed to a third party. Courts should assess the practicality of abstaining from that act as well. For instance, for many individuals, having a bank account—and therefore conveying information to a third-party bank—is necessary to function in contemporary society. Similarly, cellphones could also be considered necessary for most individuals functioning in today's society. Not having a bank

---

[238] *See* Riley v. California, 134 S. Ct. 2473, 2484, 2489–90 (2014).

[239] *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (noting that location information can reveal a "wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations").

[240] *Riley*, 134 S. Ct. at 2478 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

account or cellphone today is impractical. As Justice Marshall noted, "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[241]

Another more viable solution, at least in terms of CSLI, is a Supreme Court ruling that expressly holds that CSLI is protected by the Fourth Amendment and its procurement requires a warrant. The probable cause for a warrant standard applied to CSLI will guarantee Fourth Amendment protections as the SCA holds the government to a lesser standard.[242] No matter how courts arrive at this conclusion, they should ultimately give CSLI and similar location information Fourth Amendment protections.

CONCLUSION

Technology has developed significantly since the Fourth Amendment was ratified. It is inconceivable that the Framers could have envisioned how the Fourth Amendment would apply to location information generated from cellphones and similar devices. As such, courts are tasked with applying the Fourth Amendment to searches and seizures involving new technologies. As a result of the Supreme Court taking on this task, the reasonable expectation of privacy test and third-party doctrine has emerged. Ultimately, the circuit courts that have decided Fourth Amendment challenges to government's procurement of CSLI have wrongly applied the reasonable expectation of privacy test and the third-party doctrine. As CSLI and location information alike reveal intimate, personal details about an individual, one has a reasonable expectation of privacy in such information. Additionally, the third-party doctrine should not universally apply to CSLI or any other location information, but rather, only to information that is both *knowingly* and *voluntarily* conveyed to third parties. It is erroneous to conclude that cellphone users knowingly and voluntarily convey this information to third parties. Courts should ultimately use the

---

[241] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[242] *See* Babst, *supra* note 180, at 369; *see also In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013) ("The [SCA's] 'specific and articulable facts' standard is a lesser showing than the probable cause standard that is required by the Fourth Amendment to obtain a warrant.").

multifactor test proposed above when determining whether the third-party doctrine applies. No matter how courts come to this conclusion, such a holding is imperative to extend Fourth Amendment protections to CSLI which may reveal personal, intimate details, and that one would have an absolute reasonable expectation of privacy in.